

## Exhibit A

0300  
GEGFAMP AFI AFMEGUT  
S000UWVY  
UWU00UUAUWUVAS0US  
0300  
00U0A0F00 00 00A00

SUPERIOR COURT OF WASHINGTON IN AND FOR KING COUNTY

ANGELA HOGAN, individually and on behalf  
of all others similarly situated,

Plaintiff,

v.

AMAZON.COM, INC.,

Defendants.

No. 21-2-08004-5

CLASS ACTION COMPLAINT  
FOR DAMAGES AND INJUNCTIVE  
RELIEF

## TABLE OF CONTENTS

I.	INTRODUCTION.....	4
II.	PARTIES .....	7
III.	JURISDICTION AND VENUE .....	7
IV.	FACTUAL ALLEGATIONS .....	8
A.	Deep learning, big tech, and the road to Rekognition.....	8
1.	The rise of facial recognition through “deep learning.” .....	8
2.	Tech behemoths race to perfect image-recognition technology via deep learning .....	9
3.	Amazon makes facial-recognition technology available to consumers through Amazon Photos and to businesses and governmental entities through Rekognition.....	10
B.	Amazon Photos.....	13
1.	Through its Amazon Photos service, Amazon unlawfully collects, stores, and uses the biometric identifiers and information of Amazon Prime members residing in Illinois.....	13
2.	Amazon unlawfully collects, stores, and uses the biometric information of Illinois residents who are not Prime members but are given free Amazon Photos accounts through the Family Vault feature. ....	17
3.	Amazon unlawfully collects, stores, and uses the biometric identifiers and information of Illinois residents who have never used Amazon Photos, most of whom are unaware that Amazon has their biometric data.....	18
C.	Amazon Rekognition has raised civil-liberty and privacy concerns among civil-rights groups, members of Congress, and Amazon’s own employees and shareholders. ....	21
D.	Amazon unlawfully collected, stored, and used Plaintiff’s biometric identifiers and information through Amazon Photos.....	23
V.	CLASS ACTION ALLEGATIONS.....	24

VI.	CLAIMS FOR RELIEF.....	27
	COUNT One — Violation of Section 15(a) of Illinois’s Biometric Information Privacy Act (740 ILCS 14/15(a)) by Failing to Establish a Publicly Available Policy Governing the Retention of Biometric Identifiers and Information .....	27
	COUNT Two — Violation of Section 15(b) of Illinois’s Biometric Information Privacy Act (740 ILCS 14/15(b)) by Obtaining Biometric Identifiers or Information Without Notice or Consent .....	28
	COUNT Three — Violation of Section 15(c) of Illinois’s Biometric Information Privacy Act (740 ILCS 14/15(c)) by Profiting from Biometric Identifiers or Biometric Information Obtained Through Amazon Photos.....	30
	COUNT Four — Unjust Enrichment .....	31
VII.	PRAYER FOR RELIEF .....	32
VIII.	JURY DEMAND .....	33

1 Plaintiff Angela Hogan brings this action individually and on behalf of all others  
2 similarly situated against Defendant Amazon.com, and alleges the following based on personal  
3 knowledge, the investigation of counsel, and information and belief.

#### 4 I. INTRODUCTION

5 1. In 2008, Illinois enacted the Biometric Information Privacy Act (“BIPA” or “the  
6 Act”) with the purpose of serving “[t]he public welfare, security, and safety . . . by regulating  
7 the collection, use, safeguarding, handling, storage, retention, and destruction of biometric  
8 identifiers and information”<sup>1</sup>—namely, identifiers such as “a retina or iris scan, fingerprint,  
9 voiceprint, or scan of hand or face geometry,” and information based on those identifiers.<sup>2</sup> In so  
10 doing, the Illinois legislature recognized that “[t]he full ramifications of biometric technology  
11 are not fully known,”<sup>3</sup> and that “[b]iometrics . . . are biologically unique to the individual;  
12 therefore, once compromised, the individual has no recourse.”<sup>4</sup>

13 2. BIPA addresses the dangers posed by the mishandling of biometric identifiers  
14 and information by providing a right of action to any person who is subjected to a violation of  
15 the Act within the State of Illinois.<sup>5</sup>

16 3. As relevant here, a private entity in the possession of biometric identifiers or  
17 information violates BIPA when it (a) fails to establish a publicly available policy “establishing  
18 a retention schedule and guidelines for permanently destroying biometric identifiers and  
19 information”;<sup>6</sup> (b) obtains a person’s biometric identifier or information without first providing  
20 information”;<sup>6</sup> (b) obtains a person’s biometric identifier or information without first providing  
21 information”;<sup>6</sup> (b) obtains a person’s biometric identifier or information without first providing  
22 information”;<sup>6</sup> (b) obtains a person’s biometric identifier or information without first providing  
23 information”;<sup>6</sup> (b) obtains a person’s biometric identifier or information without first providing

---

24 <sup>1</sup> 740 ILCS 14/5(g).

25 <sup>2</sup> 740 ILCS 14/10 (defining “biometric identifier” and “biometric information”).

26 <sup>3</sup> 740 ILCS 14/5(f).

<sup>4</sup> 740 ILCS 14/5(c).

<sup>5</sup> 740 ILCS 14/20.

<sup>6</sup> 740 ILCS 14/15(a).

adequate written notice to that person and obtaining the person’s informed written consent;<sup>7</sup> or  
(c) profits in any way from the use of a person’s biometric identifiers or information.<sup>8</sup>

4. Amazon Photos (originally called Amazon Prime Photos) was launched in November 2014. A cloud-based photo storage, sharing, and organization platform, Amazon Photos provides all Amazon Prime subscribers—in Illinois and elsewhere—with “unlimited photo storage” and “enhanced search and organization features,”<sup>9</sup> including image recognition.

5. Currently, there are about 150 million Amazon Prime subscribers in the United States;<sup>10</sup> approximately 5.8 million of those subscribers reside in the State of Illinois.

6. An Amazon Prime subscription costs \$12.99 per month or \$119 per year if paid annually. Amazon therefore earns hundreds of millions of dollars a year from Illinois citizens who purchase a Prime subscription, of which Amazon Photos is one feature.

7. Amazon Photos’ image-recognition feature analyzes billions of images daily.<sup>11</sup> Each time one of those photographs contains an image of a person’s face, Amazon’s facial-recognition technology obtains that person’s biometric identifiers in the form of a “scan . . . of face geometry.”<sup>12</sup>

---

<sup>7</sup> 740 ILCS 14/15(b), 14/10.

<sup>8</sup> 740 ILCS 14/15(c).

<sup>9</sup> *What Is Amazon Photos*, AMAZON.COM (last visited June 1, 2021), <https://www.amazon.com/gp/help/customer/display.html?nodeId=G6PT8TMLM9NVZCSL>.

<sup>10</sup> *Number of Amazon Prime users in the United States from 2017 to 2022*, STATISTA (Dec. 1, 2020), <https://www.statista.com/statistics/504687/number-of-amazon-prime-subscription-households-usa/>.

<sup>11</sup> Werner Vogels, *Bringing the Magic of Amazon AI and Alexa to Apps on AWS*, ALL THINGS DISTRIBUTED (Nov. 30, 2016) (“Amazon Rekognition is a fully managed, deep learning–based image analysis service, built by [Amazon’s] computer vision scientists with the same proven technology that has already analyzed billions of images daily on Amazon Prime Photos.”), <https://www.allthingsdistributed.com/2016/11/amazon-ai-and-alexa-for-all-aws-apps.html>.

<sup>12</sup> 740 ILCS 14/10 (defining “biometric identifier”).

1           8.       The facial-recognition feature of Amazon Photos does not obtain biometric  
2 identifiers and information of only Prime subscribers who use the service; Amazon scans the  
3 facial geometry of *every* person who appears in a picture saved to Amazon Photos, regardless of  
4 whether that person is a Prime member or someone who has no idea that a photo of them has  
5 been uploaded to the platform.  
6

7           9.       Perhaps most troubling of all is that Amazon secretly uses the biometric  
8 identifiers and information of millions of people that it obtains through Amazon Photos to train  
9 and improve Rekognition<sup>13</sup>—a controversial image-recognition technology that Amazon  
10 markets and sells to numerous businesses, governmental entities, and other organizations. By  
11 improving Rekognition with the biometric identifiers and information collected through  
12 Amazon Photos, Amazon makes the product more valuable and attractive to its clients, thereby  
13 increasing its profits at the expense of the individual privacy interests that BIPA was enacted to  
14 protect.  
15

16          10.      As a private entity in the possession of biometric identifiers obtained through its  
17 facial-recognition algorithm, Amazon has violated, and continues to violate, § 15(a) of BIPA by  
18 failing to establish a publicly available policy establishing a retention schedule and guidelines  
19 for permanently destroying the biometric identifiers—namely, scans of facial geometry—  
20 obtained from pictures uploaded to Amazon Photos.<sup>14</sup> Amazon also has violated and continues  
21 to violate § 15(b) of BIPA by obtaining these facial scans without first providing adequate  
22  
23

---

24 <sup>13</sup> Becky Peterson, *Box is now plugged into Google's AI, letting you easily search through images without needing*  
25 *to first tag them*, BUSINESS INSIDER (Aug. 17, 2017) (“Amazon’s Rekognition . . . was trained by analyzing the  
26 billions of images uploaded daily into Prime Photos.”), <https://www.businessinsider.in/box-is-now-plugged-into-googles-ai-letting-you-easily-search-through-images-without-needing-to-first-tag-them/articleshow/60107339.cms>.

<sup>14</sup> 740 ILCS 14/15(a).

1 written notice and obtaining written informed consent from persons appearing in the uploaded  
2 photos, including Plaintiff and Class Members.<sup>15</sup>

3 11. Amazon has violated and continues to violate § 15(c) of BIPA by wrongfully  
4 profiting from the billions of facial scans it has collected through its Photos platform—including  
5 facial scans Plaintiff and Class Members—by using the biometric information it obtains from  
6 Amazon Photos to improve Rekognition, thereby making the technology more profitable to  
7 Amazon, which sells Rekognition to businesses, law enforcement agencies, and other entities.

8 12. In sum, Amazon obtained images of Plaintiff and Class Members through the  
9 Amazon Photos platform and then wrongfully collected and profited from their biometric  
10 identifiers and information, thereby harming the substantive privacy interests that the Biometric  
11 Information Privacy Act was intended to protect.  
12

## 13 **II. PARTIES**

14 13. Plaintiff Hogan is a natural person and a citizen of the State of Illinois.

15 14. Defendant Amazon.com, Inc. is a Delaware corporation with a principal place of  
16 business at 410 Terry Avenue North, Seattle, Washington 98109-5210.  
17

## 18 **III. JURISDICTION AND VENUE**

19 15. This Court has subject matter jurisdiction under RCW § 2.08.100.

20 16. This Court has personal jurisdiction over Defendant Amazon because its  
21 principal place of business is in in King County.  
22

23 17. Venue is proper under RCW § 4.12.020(3) because Defendant Amazon's  
24 corporate residence is in King County.<sup>16</sup>  
25

---

26 <sup>15</sup> 740 ILCS 14/15(b).

<sup>16</sup> See RCW § 4.12.025(1) (defining corporate residence for venue purposes).



#### IV. FACTUAL ALLEGATIONS

##### A. Deep learning, big tech, and the road to Rekognition.

##### 1. The rise of facial recognition through “deep learning.”

18. In general, “facial recognition” refers to the scanning of a person’s face and matching it against a library of facial images. Facial recognition is a type of “image recognition”—a term that refers more broadly to computer technologies that can recognize people, animals, objects, or other targeted subjects using algorithms and machine learning.

19. Many of the recent advances in image-recognition technologies rely “on deep learning technology, an advanced type of machine learning and artificial intelligence.”<sup>17</sup> Deep learning “works by building deep neural networks that simulate the mechanism of the human brain and then interpreting and analyzing data, such as image, video and text.”<sup>18</sup>

20. Unlike other machine-learning algorithms, “[d]eep learning networks do not require human intervention because the nested algorithms run the data through different concepts which eventually learn from their own mistakes.”<sup>19</sup> Thus, “[d]eep learning is suitable for instances where there are boatloads of data to analyze or complex problems to solve.”<sup>20</sup>

21. This makes deep-learning networks particularly well suited to (among other things) image recognition, including facial recognition: “Face recognition leverages computer vision to extract discriminative information from facial images and deep learning techniques to

---

<sup>17</sup> Christine Facciolo, *The future of image recognition technology is deep learning*, TECHNICAL.LY (Sept. 20, 2019), <https://technical.ly/dc/2019/09/20/image-recognition-technology-artificial-intelligence/>.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

1 model the appearances of faces, classify them and transmit the data. Algorithms extract facial  
 2 features and compare them to a database to find the best match.”<sup>21</sup>

3 **2. Tech behemoths race to perfect image-recognition technology via deep**  
 4 **learning.**

5 22. In 2014—the year that Amazon launched Amazon Photos—image recognition  
 6 was being touted as “the tech world’s ‘next big thing,’” in large part because of advances in  
 7 deep learning.<sup>22</sup> At the time, image-recognition technology had been in development for  
 8 decades,<sup>23</sup> but Silicon Valley technology companies had only recently begun devoting immense  
 9 resources to the development of such technology “to make the most of the vast amounts of data  
 10 [including photos] that data users share with them.”<sup>24</sup>

11 23. Facebook made a “big push” into image-recognition technology by purchasing  
 12 the facial-recognition startup Face.com in 2012.<sup>25</sup> Only two years later, Facebook unveiled  
 13 DeepFace, a deep-learning network that could purportedly “determine whether two  
 14 photographed faces are of the same person with 97.25 percent accuracy.”<sup>26</sup> By early 2015,  
 15 Facebook had begun using DeepFace to identify and tag its users in photos uploaded to  
 16 Facebook.<sup>27</sup>

17  
 18  
 19 

---

 20 <sup>21</sup> *Id.*

21 <sup>22</sup> Jess Bolluyt, *Why Image Recognition Is the Tech World’s ‘Next Big Thing,’* CHEATSHEET.COM (Sept. 14, 2014)  
 22 (“Google’s focus on deep learning, and explorations of its potential for image recognition, runs parallel to what  
 23 other companies in Silicon Valley are researching.”), [https://www.cheatsheet.com/technology/why-image-  
 24 recognition-is-the-tech-worlds-next-big-thing.html/](https://www.cheatsheet.com/technology/why-image-recognition-is-the-tech-worlds-next-big-thing.html/).

25 <sup>23</sup> *The History of Face Recognition*, FACEFIRST BLOG (last visited June 1f, 2021),  
 26 <https://www.facefirst.com/blog/brief-history-of-face-recognition-software/>.

<sup>24</sup> Bolluyt, *supra* note 22.

<sup>25</sup> Kate Knibbs, *Inside Facebook’s freakishly accurate face recognition technology*, DAILY DOT (Mar. 2, 2020),  
<https://www.dailydot.com/debug/facebook-facial-recognition-deepface/>.

<sup>26</sup> Dino Grandoni, *Facebook’s New ‘DeepFace’ Program Is Just As Creepy As It Sounds*, HUFFINGTON POST  
 (Mar. 18, 2014), [https://www.huffpost.com/entry/facebook-deepface-facial-recognition\\_n\\_4985925](https://www.huffpost.com/entry/facebook-deepface-facial-recognition_n_4985925).

<sup>27</sup> Victoria Woolaston, *Facebook can tag you in photos AUTOMATICALLY: Social network starts rolling out DeepFace recognition feature*, THE DAILY MAIL (Feb. 9, 2015), [https://www.dailymail.co.uk/sciencetech/article-  
 2946186/Facebook-soon-tag-photos-AUTOMATICALLY-Social-network-starts-rolling-DeepFace-feature.html](https://www.dailymail.co.uk/sciencetech/article-2946186/Facebook-soon-tag-photos-AUTOMATICALLY-Social-network-starts-rolling-DeepFace-feature.html).

24. For its part, “Google started [an] acquisition spree in late 2012 with facial recognition company Viewdle and . . . continued picking up [other] neural networks.”<sup>28</sup> By early 2015, Google was touting its own deep-learning facial-recognition system, called FaceNet, as “the most-accurate technology available for recognizing human faces,” claiming that it “achieve[d] a new record accuracy of 99.63%” in face-matching.<sup>29</sup>

25. In 2015, Apple acquired the startup Perception, which “focuse[d] on image-based recognition and deep learning,”<sup>30</sup> and in 2016 early acquired Emotient, “an artificial intelligence startup that reads people’s emotions by analysing facial expressions.”<sup>31</sup> By mid-2016, Apple had updated its Photos app to incorporate “advanced computer vision, a group of deep learning techniques that [brought] facial recognition to the iPhone.”<sup>32</sup>

### 3. Amazon makes facial-recognition technology available to consumers through Amazon Photos and to businesses and governmental entities through Rekognition.

26. Amazon lagged slightly behind other tech giants in its development of facial-recognition technology but caught up quickly. In the fall of 2015, Amazon acquired the deep-learning startup Orbeus, Inc.—which had developed the PhotoTime app for both Apple’s iOS and Google’s Android operating system—and hired nearly all its personnel.<sup>33</sup>

<sup>28</sup> Dan Rowinski, *Google’s Game Of Moneyball In The Age Of Artificial Intelligence*, READWRITE (Jan. 29, 2014), <https://readwrite.com/2014/01/29/google-artificial-intelligence-robots-cognitive-computing-moneyball/>.

<sup>29</sup> Matt Prigg, *Google claims its ‘FaceNet’ system has almost perfected recognising human faces – and is accurate 99.96% of the time*, THE DAILY MAIL (Mar. 19, 2015), <https://www.dailymail.co.uk/sciencetech/article-3003053/Google-claims-FaceNet-perfected-recognising-human-faces-accurate-99-96-time.html>.

<sup>30</sup> Nathan Eddy, *Apple Acquires Perception, A Deep Learning, AI Specialist*, INFORMATIONWEEK (Oct. 6, 2015), <https://www.informationweek.com/mobile/mobile-applications/apple-acquires-perceptio-a-deep-learning-ai-specialist/d/d-id/1322502>.

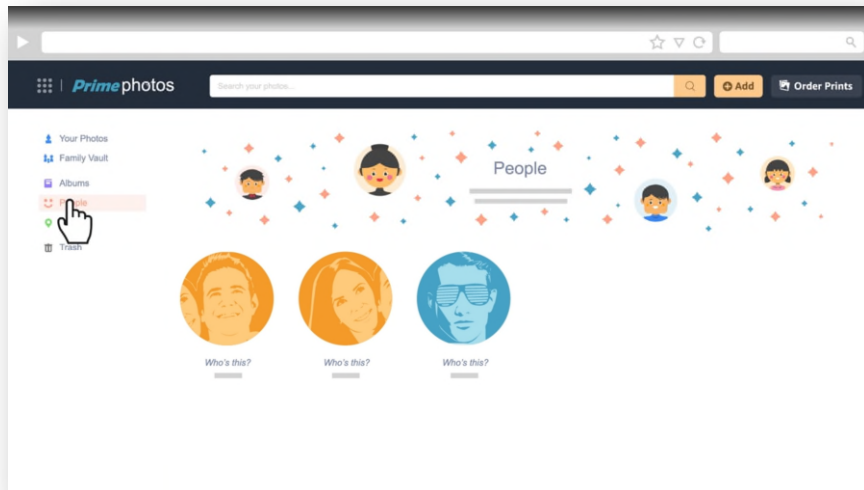
<sup>31</sup> *Apple Buys Artificial Intelligence Startup Emotient: Report*, GADGETS 360 (Jan. 8, 2016), <https://gadgets.ndtv.com/internet/news/apple-buys-artificial-intelligence-startup-emotient-report-787123>.

<sup>32</sup> Bryan Clark, *Apple brings Google-style machine learning to ‘Photos,’* TNW (June 13, 2016), <https://thenextweb.com/apple/2016/06/13/apple-brings-google-style-machine-learning-to-photos/>.

<sup>33</sup> Rob Thubron, *Amazon quietly acquired AI image analysis startup Orbeus late last year*, TECHSPOT (Apr. 6, 2016), <https://www.techspot.com/news/64358-amazon-quietly-acquired-ai-image-analysis-startup-orbeus.html>;

27. The PhotoTime app developed by Orbeus could “detect, tag, and sort features in photos, including objects, faces, scenes, and time.”<sup>34</sup> PhotoTime was “based on Orbeus’ ReKognition API [application-programming interface], which allowed other developers to build apps that use[d] the same photo-recognition technology.”<sup>35</sup> Once Orbeus was acquired by Amazon, however, ReKognition was no longer available to new customers.<sup>36</sup>

28. By late 2016—a year after its acquisition of Orbeus—Amazon had integrated the image-recognition technology it had acquired into Amazon Photos.<sup>37</sup> Users of Amazon Photos were now able to find images of family members and friends in their uploaded photos,<sup>38</sup> as images of the same person are grouped together automatically using facial recognition:<sup>39</sup>



Jordan Novet, *Amazon hires team behind deep learning startup Orbeus*, VENTUREBEAT (Apr. 5, 2016), <https://venturebeat.com/2016/04/05/amazon-orbeus-deep-learning/>.

<sup>34</sup> Thubron, *supra* note 33.

<sup>35</sup> Thubron, *supra* note 33.

<sup>36</sup> Thubron, *supra* note 33.

<sup>37</sup> Ken Yeung, *Amazon's Prime Photos service now lets you share storage with 5 family members*, VENTUREBEAT (Oct. 18, 2016), <https://venturebeat.com/2016/10/18/amazons-prime-photos-service-now-lets-you-share-storage-with-5-family-members/>.

<sup>38</sup> *Id.*

<sup>39</sup> *Video: How Does Image Recognition Work*, AMAZON (last visited June 1, 2021), available at <https://www.amazon.com/gp/help/customer/display.html?nodeId=G3BC9SVPPEVSB9T8>.

29. Then, in January 2017, Amazon launched Rekognition—an updated version of the ReKognition (with a capital K) deep-learning application-programming interface it had acquired in 2015. Amazon markets and sells Rekognition technology to businesses, governmental entities, and other organizations through Amazon Web Services,<sup>40</sup> a cloud-based platform that today offers 200 services globally<sup>41</sup>—including, among other things, cloud-based storage, analytics, management tools, security, and various “enterprise applications.”<sup>42</sup>

30. Amazon publicly acknowledged at the time that it had “been using Rekognition within its Amazon Prime Photo service.”<sup>43</sup>

31. What Amazon users and the public were *not* told, however, was that Amazon’s deep-learning Rekognition technology was “trained by analyzing the billions of images uploaded daily into Prime Photos.”<sup>44</sup>

32. In other words, the biometric identifiers—scans of facial geometry—of untold millions of people were obtained, stored, and analyzed by Amazon’s Rekognition from the billions of images uploaded to Amazon Photos daily. The ability to “learn” from all of the images stored in Amazon Photos accounts made Rekognition more accurate. This, in turn, made Rekognition more valuable to Amazon’s business, governmental, and organizational customers, enabling Amazon to profit from the biometric identifiers and information of not only millions of

---

<sup>40</sup> Kent Weare, *Amazon Introduces Rekognition for Image Analysis*, INFOQ (Jan. 8, 2017), <https://www.infoq.com/news/2017/01/AWS-Rekognition/>.

<sup>41</sup> *What is AWS*, AWS (last visited June 1, 2021), <https://aws.amazon.com/what-is-aws/>.

<sup>42</sup> *Cloud Products*, AWS (last visited June 1, 2021), <https://aws.amazon.com/products/>.

<sup>43</sup> Weare, *supra* note 40; *see also* Shudeep Chandrasekhar, 1REDDROP (Dec. 4, 2016) (explaining that Rekognition “is a technology that Amazon itself uses – for Prime Photos”), <https://1reddrop.com/2016/12/04/amazons-biggest-contribution-artificial-intelligence-application-developers/>; Nancy Cohen, *Amazon improves face analysis tech, adds fear*, TECH XPLORE (Aug. 15, 2019) (“‘Rekognition Image is based on the same proven, highly scalable, deep learning technology developed by Amazon’s computer vision scientists to analyze billions of images daily for Prime Photos,’ said the company [Amazon].”), <https://techxplore.com/news/2019-08-amazon-analysis-tech.html>.

<sup>44</sup> Peterson, *supra* note 13.

1 Prime customers but also millions of *non*-Prime customers whose images were uploaded to  
2 Amazon Photos, often without their knowledge or consent.

3 **B. Amazon Photos**

4 **1. Through its Amazon Photos service, Amazon unlawfully collects, stores, and uses**  
5 **the biometric identifiers and information of Amazon Prime members residing in**  
6 **Illinois.**

7 33. Amazon is the world’s largest online retailer and recently became the largest  
8 retailer (online or otherwise) in the world, surpassing Walmart. The company offers consumers  
9 membership to its Amazon Prime service for \$12.99 a month. Prime members have access to  
10 faster and cheaper shipping options, exclusive discounts, and a host of Amazon’s online  
11 services, including Prime Video, Amazon Music, and Prime Photos.

12 34. Prime Photos is a cloud-based platform that provides members with unlimited  
13 online storage of full-resolution photos. The Prime Photos app—available on Windows,  
14 Android, and iOS devices—enables members to automatically upload all of their digital photos  
15 to the cloud (namely, Amazon’s servers).<sup>45</sup>

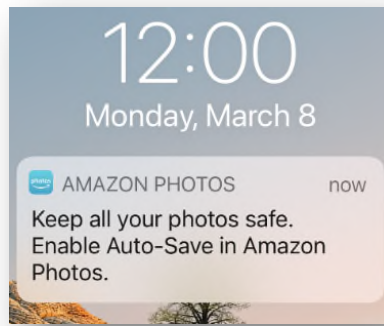
16 35. A Prime member who has installed the Photos app on their mobile phone can  
17 take a picture with their phone’s camera and have that picture instantaneously stored on  
18 Amazon’s servers, making the picture accessible from any internet-enabled device anywhere in  
19 the world.  
20

21 36. Users who do not have the “auto-save” feature enabled are continually prodded  
22 by the app to do so:  
23  
24  
25

26 

---

<sup>45</sup> *What is Amazon Photos?*, AMAZON (May 8, 2019), <https://www.amazon.com/primeinsider/tips/prime-photos-qa.html>.



37. Image- and facial-recognition technology (Rekognition) is integrated into Amazon Photos, so that “the app organizes your photos automatically. You can quickly find any specific photo by searching for a particular date, or by people and things in their images, like ‘dog’ or ‘sunset.’ You can also organize your photos in albums.”<sup>46</sup> Amazon represents that “[t]he best part is that all this organization happens automatically, without you lifting a finger.”<sup>47</sup>

38. The Amazon Photos terms of use state that “[i]mage recognition features are enabled automatically when you begin using the Services unless the billing information associated with your account indicates that you may be an Illinois resident, in which case the image recognition features will be disabled and must be enabled by you.”<sup>48</sup>

39. Although the image-recognition features of Photos are not automatically enabled for Prime members who are Illinois residents, the Amazon Photos app prompts Illinois residents to enable image recognition:

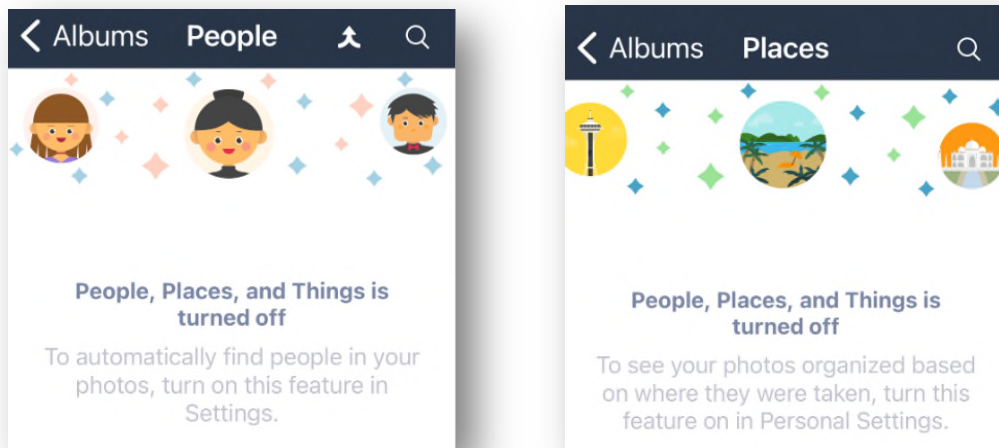
---

<sup>46</sup> *Id.*

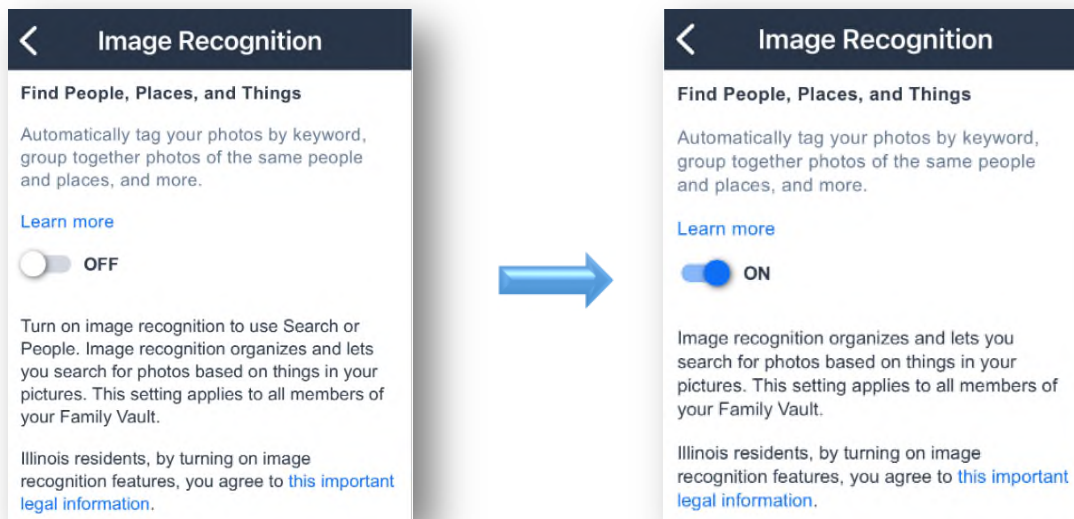
<sup>47</sup> *Id.*

<sup>48</sup> *Amazon Photos Terms of Use*, AMAZON (last updated June 1, 2020), <https://www.amazon.com/gp/help/customer/display.html?nodeId=201376540>.





40. Moreover, a user can readily enable the image-recognition feature with one tap of a finger:



41. As these images show, there is a statement at the bottom of the screen telling Illinois residents that, “by turning on image recognition features, you agree to this important legal information.” While the user has the option of clicking on a hyperlink to visit a page with the “important legal information,” the user can enable image recognition without doing so.



42. Users who do click on the hyperlink are taken to a page stating that “an Illinois state law *may* require the informed written consent from an Illinois resident before performing image recognition on photos that include his or her face.”<sup>49</sup> The page also falsely represents that it is the responsibility of the Prime subscriber—not Amazon—to obtain informed written consent from “the individuals in the photos stored in [their] account” before collecting those individuals’ biometric identifiers or information:<sup>50</sup>

Image recognition features are disabled initially for Illinois residents because an Illinois state law may require the informed written consent from an Illinois resident before performing image recognition on photos that include his or her face.

**Enabling Image Recognition on Photos.** By enabling image recognition features for your account, you understand that image recognition analysis will be performed on the photos stored in your account, and you represent to us that you have obtained the consent of the individuals in the photos stored in your account permitting us to use image recognition analysis on photos of them.

43. Of course, Amazon knows that very few—if any—account holders go through the trouble of confirming that every friend, family member, or other person who is in their photos provides the informed consent that is necessary for Amazon to collect their biometric identifiers and information.

44. Moreover, Amazon does nothing to confirm that Prime subscribers are in fact legally authorized representatives of the non-account holders whose images are saved to Amazon Photos and scanned using facial-recognition technology.

45. Neither the account holder nor any other person whose image is uploaded to Amazon Photos is ever informed—either on the “notice” page or in the Amazon Photos terms of

<sup>49</sup> *Notice to Illinois Residents*, AMAZON (last visited June 1, 2021) (emphasis added), <https://www.amazon.com/gp/help/customer/display.html?nodeId=202094310>.

<sup>50</sup> *Id.*

use<sup>51</sup>—that one of the main purposes of Amazon’s collecting, storing, and using the facial scans of persons in the stored photos is to improve Amazon’s Rekognition technology.<sup>52</sup> In this way, the biometric identifiers and information collected through the Photos platform enable Amazon to reap bigger profits from selling its image-recognition service Rekognition to businesses, governmental entities, and other organizations.

**2. Amazon unlawfully collects, stores, and uses the biometric information of Illinois residents who are not Prime members but are given free Amazon Photos accounts through the Family Vault feature.**

46. Prime members are not the only consumers with access to the Amazon Photos service. Any Prime subscriber based in the United States can provide free Amazon Photos accounts to up to five people by inviting them to a “Family Vault.”

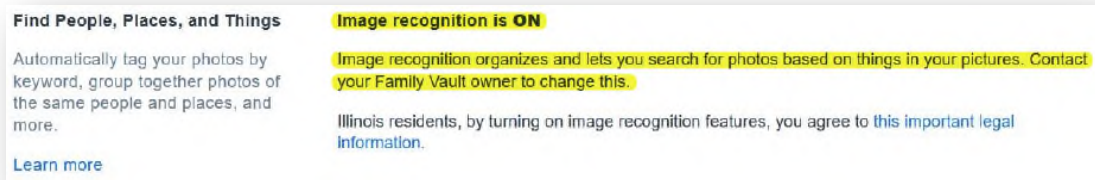
47. A person who accepts an invitation to join a Family Vault receives a free Amazon Photos account even if they are not a Prime member. Like the Prime member who invited them, the “Vault member” can store unlimited full-resolution photos in their Amazon Photos account and has full access to many features such as auto-save.

48. There is one important Photos feature that a Vault member does *not* have access to. If the Prime member who invited them to a Family Vault has image recognition enabled, the Vault member *cannot* disable the image-recognition feature in their own Amazon Photos account:

---

<sup>51</sup> See *id.*; *Amazon Photos Terms of Use*, AMAZON (last updated May 3, 2021), <https://www.amazon.com/gp/help/customer/display.html?nodeId=201376540>.

<sup>52</sup> See 740 ILCS 14/15(b)(2) (providing that private entity that obtains a person’s biometric identifier or information must “inform[ ] the subject or their legally authorized representative in writing of the *specific purpose* and length of term for which a biometric identifier or biometric information is being collected, stored, and used” (emphasis added)).



49. Image recognition is enabled by default for Prime members who do not reside in Illinois,<sup>53</sup> and most users never disable the feature (many because they are unaware of it).

50. Image recognition is therefore permanently enabled for most Vault members' accounts—including the accounts of those Vault members who reside in Illinois.

51. Amazon obtains the biometric identifiers and information of every persons whose images are stored in those accounts by scanning their facial geometry.

**3. Amazon unlawfully collects, stores, and uses the biometric identifiers and information of Illinois residents who have never used Amazon Photos, most of whom are unaware that Amazon has their biometric data.**

52. Amazon collects and profits from the biometric identifiers and information of millions of people who do not have an Amazon Photos account. Indeed, a person's biometric data is collected through Amazon photos regardless of whether that person has purchased anything from Amazon, is aware that their image is stored by Amazon Photos, or has ever even heard of Amazon Photos.

53. There are countless ways that this can occur, including:

- a. An Amazon Photos account holder (whether a Prime member or Vault member) takes a street photo that captures pedestrians the account holder does not know, and the photo is automatically stored in Amazon Photos via the Photos app on the account holder's phone.

<sup>53</sup> See *How Does Image Recognition Work?*, AMAZON (last visited June 1, 2021) ("Image recognition in Amazon Photos is enabled by default, unless you are a resident of Illinois."), <https://www.amazon.com/gp/help/customer/display.html?nodeId=G3BC9SVPPEVSB9T8>.

- b. An account holder takes a picture at a family reunion. Again, the picture is automatically stored in Amazon Photos without the knowledge or consent of the persons in the photo.
- c. An account holder takes numerous photos at their child's birthday party. Numerous children are in the photos, and the photos are stored automatically in Amazon Photos without the knowledge of the children or their parents.
- d. An account holder takes a selfie at a bar, with several strangers in the background. Those strangers' images are automatically stored in Amazon Photos.

54. In each of the above examples, if image recognition is enabled in the Photos account, the persons who unwittingly appear in the uploaded photos have their facial geometry scanned by Amazon without their knowledge, let alone their informed written consent. Amazon profits from these persons' biometric identifiers and information by using this biometric data to improve the Rekognition technology that Amazon sells to businesses, governmental entities, and other organizations.

55. Moreover, it is unclear how long Amazon retains the biometric identifiers and information derived from the photos stored in Amazon Photos, and how long it continues to profit from them.

56. Section 15(a) of BIPA requires that Amazon have a publicly available written policy "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."<sup>54</sup>

57. The Amazon Photos terms of use tells account holders that Amazon:

---

<sup>54</sup> 740 ILCS 14/15(a).

1 retain[s] image recognition data, including data about the faces, in the photos you  
2 store using the Services until you disable the image recognition features or your  
3 account's access to the Services is terminated. If your image recognition features  
4 are disabled, we will stop storing image recognition data for you, and we will not  
5 tag any new photos uploaded to your account.<sup>55</sup>

6 58. This statement in the terms of use does not explain what is encompassed by the  
7 term "image recognition data." As recognized by courts, "biometric information" for which a  
8 retention schedule must be made publicly available is broadly defined in BIPA<sup>56</sup> to prevent  
9 private entities from evading "the Act's restrictions by converting a person's biometric identifier  
10 into some other piece of information, like a mathematical representation or, even simpler, a  
11 unique number assigned to a person's biometric identifier."<sup>57</sup> Thus, "whatever a private entity  
12 does in manipulating a biometric identifier into a piece of information, the resulting information  
13 is still covered by the Privacy Act if that information can be used to identify the person."<sup>58</sup>

14 59. Amazon does not disclose to users or the public that it uses the biometric  
15 identifiers and information obtained through Amazon Photos to train its Rekognition  
16 technology. And there is no way to know what manipulations the collected biometric identifiers  
17 undergo before and after being used to train Amazon's Rekognition technology.

18 60. The statement in the terms of use also falls short because non-account holders  
19 have not had an interaction with Amazon related to Amazon Photos' collection of their  
20 biometric identifiers and information. Thus, Amazon violates § 15(a) the moment it obtains  
21 biometric identifiers and information of a non-account holder. Because Amazon has had no  
22

---

23  
24 <sup>55</sup> *Amazon Photos Terms of Use*, AMAZON (last updated May 3, 2021), <https://www.amazon.com/gp/help/customer/display.html?nodeId=201376540>.

25 <sup>56</sup> See 740 ILCS 14/4 ("'Biometric information' means any information, regardless of how it is captured,  
26 converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.").

<sup>57</sup> *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017).

<sup>58</sup> *Id.*

relevant interaction with non-account holders, Amazon *cannot* satisfy the requirement of destroying their biometric data “within 3 years of the individual’s last interaction” with Amazon.

**C. Amazon Rekognition has raised civil-liberty and privacy concerns among civil-rights groups, members of Congress, and Amazon’s own employees and shareholders.**

61. Since launching its deep-learning image-recognition service Rekognition, Amazon has marketed and sold access to the technology to numerous businesses, including C-SPAN, Marinus Analytics, Aella Credit, Kyodo News, Mainichi Newspapers, K-STAR Group, POPSUGAR Inc., FamilySearch, Sen Corporation, CampSite, Wia, OneFi, Woo, CA Mobile Inc., Uluru, and ARMED Inc.,<sup>59</sup> as well as to numerous governmental entities, including U.S. Immigration and Customs Enforcement and an unknown number of police departments across the United States.<sup>60</sup>

62. All the while, Amazon was using, and continues to use, the biometric identifiers and information from facial images stored by consumers in Amazon Photos to train the Rekognition algorithm.<sup>61</sup>

63. By mid-2018, civil- and privacy-rights organizations like the ACLU were raising concerns about the use of Rekognition technology, particularly by governmental entities. The ACLU called on Amazon to “stop selling facial-recognition software to government entities like the Portland-area county, which has used the cloud-computing service to compare images of

---

<sup>59</sup> *Amazon Rekognition Customers*, AMAZON (last visited June 1, 2021), <https://aws.amazon.com/rekognition/customers/>.

<sup>60</sup> Ben Gilbert, *Amazon sells facial recognition software to police all over the US, but has no idea how many departments are using it*, BUSINESS INSIDER (Feb. 21, 2020), <https://www.businessinsider.com/amazon-rekognition-police-use-unknown-2020-2>.

<sup>61</sup> See, e.g., Peterson, *supra* note 13 (“Amazon’s Rekognition . . . was trained by analyzing the billions of images uploaded daily into Prime Photos.”).

1 people in public places to its database of criminal suspects.”<sup>62</sup> The ACLU’s letter to Amazon  
 2 CEO Jeff Bezos articulated the privacy concerns presented by governments’ use of Rekognition:  
 3 “People should be free to walk down the street without being watched by the government. . . .  
 4 Facial recognition in American communities threatens this freedom.”<sup>63</sup>

5  
 6 64. Around the same time, the ACLU tested Rekognition, having it “compare official  
 7 photos of every member of the U.S. House and Senate against a database of 25,000 public arrest  
 8 photos.”<sup>64</sup> Rekognition “found ‘matches’ for 28 members of Congress with at least 80 percent  
 9 confidence, Amazon’s default setting,” and the matches “were disproportionately people of  
 10 colour.”<sup>65</sup>

11 65. In early 2019, an MIT study raised additional civil-liberties concerns, finding  
 12 “that Rekognition may have gender and racial biases”:

13  
 14 When the software was presented with a number of female faces, it incorrectly  
 15 labeled 19 percent of them as male.

16 But the outcome was much worse for darker-skinned women.

17 Of the dark-skinned women it was presented, Rekognition incorrectly labeled 31  
 18 percent of them as men.<sup>66</sup>

19 66. Following the release of the MIT report, “civil liberties groups, members of  
 20 Congress and Amazon’s own employees, [as well as] a group of shareholders [called on

21 <sup>62</sup> Matt Day, *ACLU asks Amazon to stop selling facial-recognition tools to governments*, THE SEATTLE TIMES  
 22 (May 23, 2018), [https://www.seattletimes.com/business/amazon/aclu-asks-amazon-to-stop-selling-facial-](https://www.seattletimes.com/business/amazon/aclu-asks-amazon-to-stop-selling-facial-recognition-tools-to-governments/)  
 23 [recognition-tools-to-governments/](https://www.seattletimes.com/business/amazon/aclu-asks-amazon-to-stop-selling-facial-recognition-tools-to-governments/).

24 <sup>63</sup> *ACLU asks Amazon to stop marketing face-recognition technology to police*, LOS ANGELES TIMES (May 22,  
 25 2018), <https://www.latimes.com/business/technology/la-fi-tn-amazon-facial-recognition-20180522-story.html>.

26 <sup>64</sup> Jeffrey Dastin, *Amazon’s face ID tool mismatched 28 members of Congress to mug shots – ACLU*, REUTERS  
 (July 26, 2018), <https://www.reuters.com/article/uk-amazon-com-facial-recognition-idUKKBN1KG1K9>.

<sup>65</sup> *Id.*

<sup>66</sup> Annie Palmer, *Amazon’s controversial facial recognition software can’t tell the difference between men and women or recognize dark-skinned females, MIT study finds*, THE DAILY MAIL (Jan. 25, 2019), [https://www.dailymail.co.uk/sciencetech/article-6633569/Amazons-facial-recognition-software-mistakes-women-](https://www.dailymail.co.uk/sciencetech/article-6633569/Amazons-facial-recognition-software-mistakes-women-men-darker-skinned-women-men.html)  
[men-darker-skinned-women-men.html](https://www.dailymail.co.uk/sciencetech/article-6633569/Amazons-facial-recognition-software-mistakes-women-men-darker-skinned-women-men.html).



1 Amazon] to stop selling its Rekognition technology to government agencies.”<sup>67</sup> Amazon refused  
2 to make any changes to Rekognition.<sup>68</sup>

3 67. Finally, in June 2020, Amazon announced that it was “implementing a one-year  
4 moratorium on police use of Amazon’s facial recognition technology.”<sup>69</sup> There is no indication  
5 that Amazon has stopped selling its facial-recognition technology to businesses, non-profits, and  
6 governmental entities that are not police departments.

7 68. The concerns about Amazon’s Rekognition echo the Illinois General Assembly’s  
8 finding, in enacting BIPA, that “[a]n overwhelming majority of members of the public are  
9 weary of the use of biometrics when such information is tied to . . . personal information,”<sup>70</sup> and  
10 the Assembly’s concern that “[t]he full ramifications of biometric technology are not fully  
11 known.”<sup>71</sup>

12  
13  
14 **D. Amazon unlawfully collected, stored, and used Plaintiff’s biometric identifiers and  
information through Amazon Photos.**

15 69. In approximately January 2021, Plaintiff began using the Amazon Photos  
16 service, which was available to her through her Amazon Prime subscription.

17 70. Image recognition is enabled in Plaintiff’s Amazon Photos account, although  
18 Plaintiff does not recall ever enabling the feature.  
19  
20  
21  
22

---

23 <sup>67</sup> Alfred Ng, *Shareholders demand Amazon end facial recognition sales to government*, CNET (Jan. 17, 2019),  
24 <https://www.cnet.com/news/shareholders-demand-amazon-end-facial-recognition-sales-to-government/>.

<sup>68</sup> Palmer, *supra* note 66.

25 <sup>69</sup> *We are implementing a one-year moratorium on police use of Rekognition*, AMAZON (June 10, 2020),  
26 <https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition>.

<sup>70</sup> 740 ILCS 14/5(d).

<sup>71</sup> 740 ILCS 14/5(f).



1           71.     Images of Plaintiff are stored in her Amazon Photos account. Because the  
2 image-recognition feature on the account is enabled, Amazon has scanned Plaintiff's facial  
3 geometry, thereby collecting and storing Plaintiff's biometric identifiers and information.

4           72.     Plaintiff has never received or seen any information from Amazon stating how  
5 long the biometric data obtained from her Amazon Photos account would be retained by  
6 Amazon.

7           73.     Plaintiff has never received or seen any guidelines for when or how the biometric  
8 data collected from the Amazon Photos account would be destroyed by Amazon.

9           74.     Amazon never informed Plaintiff of the specific purpose or length of time that  
10 the biometric data collected from the images in the Amazon Photos account would be collected,  
11 stored, or used. Among other things, Amazon never informed Plaintiff that that this biometric  
12 data would be used to improve Amazon's Rekognition technology, which Amazon sells to third  
13 parties at a profit.

14           75.     Plaintiff never executed a written release stating that Amazon could use her  
15 biometric data to improve the Rekognition technology it sells to businesses and other entities.

## 16                               **V.     CLASS ACTION ALLEGATIONS**

17           76.     Plaintiff Angela Hogan brings this action on behalf of herself and under CR 23,  
18 as a representative of a Class defined as follows:

19                   All Illinois citizens who, while residing in the state of Illinois, had their biometric  
20 identifiers—including scans of facial geometry and related biometric  
21 information—collected, captured, received, or otherwise obtained by Amazon  
22 from photographs uploaded to an Amazon Photos account for which they were  
23 the account holder.  
24

1           77. Excluded from the Class are Defendant Amazon and any entity in which  
2 Defendant has a controlling interest, as well as any of Defendant's legal representatives,  
3 officers, directors, assignees, and successors.

4           78. **Numerosity.** Members of the Class are so numerous that joinder of all Class  
5 Members is impractical. Currently, there are about 150 million Amazon Prime subscribers in the  
6 United States,<sup>72</sup> and approximately 5.8 million of those subscribers reside in the State of Illinois.  
7 Thus, by conservative estimates Class Members number in the tens or hundreds of thousands.  
8 Class Members are readily identifiable from information and records in Amazon's possession.  
9

10           79. **Typicality.** Plaintiff's claims are typical of the claims of the members of the  
11 Class. Plaintiff and Class Members were aggrieved by the same wrongful conduct of Amazon:  
12 their substantive privacy interests were harmed by Amazon's failure to establish an adequate  
13 publicly available policy regarding the retention of Class Members' biometric identifiers and  
14 information, by Amazon's obtains their biometric identifiers or information without first  
15 providing adequate written notice their informed written consent, and by Amazon's profiting  
16 from their biometric identifiers or information.<sup>73</sup>  
17

18           80. **Adequacy.** Plaintiff will fairly and adequately protect and represent the interests  
19 of the Class. The interests of Plaintiff are coincident with, and not antagonistic to, those of the  
20 other members of the Class. Plaintiff is represented by counsel with experience in the  
21 prosecution of class actions and with particular experience with class actions raising claims  
22 under BIPA.  
23

24  
25  
26 <sup>72</sup> *Number of Amazon Prime users in the United States from 2017 to 2022*, STATISTA (Dec. 1, 2020),  
<https://www.statista.com/statistics/504687/number-of-amazon-prime-subscription-households-usa/>.

<sup>73</sup> 740 ILCS 14/15(c).

1           81.     **Commonality and Predominance.** Questions of law and fact common to the  
2 members of the Class predominate over questions that may affect only individual Class  
3 Members because Amazon has acted on grounds generally applicable to the entire Class,  
4 thereby making damages with respect to the Class as a whole appropriate. Such generally  
5 applicable conduct is inherent in Amazon's wrongful actions. Questions of law and fact  
6 common to the Class include:  
7

8           A.     Whether Amazon established a publicly available policy for retention of  
9 biometric identifiers and information sufficient to satisfy the requirements of  
§ 15(a) of BIPA.

10          B.     Whether Amazon provided written notice and obtained written consent of  
11 persons whose biometric identifiers and information were collected by Amazon  
12 Photos' facial-recognition algorithm and, if so, whether such notice and consent  
are sufficient to satisfy the requirements of § 15(b) of BIPA.

13          C.     Whether Amazon profited from the use of the biometric identifiers and  
14 information it collected via Amazon Photos by using that biometric data to train  
15 the Rekognition technology it sold to businesses, governmental entities, and  
other organizations.

16          D.     Whether Amazon's treatment of the biometric identifiers and information  
17 collected via Amazon Photos was negligent, intentional, or reckless.

18          E.     Whether persons who had their biometric identifiers and information  
19 collected via Amazon Photos are entitled to damages and, if so, in what amount.

20          F.     Whether Amazon should be enjoined from collecting biometric identifiers  
and information through the Amazon Photos service.

21           82.     **Superiority of Class Action.** Class-action treatment is a superior method for the  
22 fair and efficient adjudication of the controversy. Such treatment will permit a large number of  
23 similarly situated persons to prosecute their common claims in a single forum simultaneously,  
24 efficiently, and without the unnecessary duplication of evidence, effort, or expense that  
25 numerous individual actions would engender. The benefits of proceeding through the class  
26 mechanism, including providing injured persons or entities a method for obtaining redress on

1 claims that could not practicably be pursued individually, substantially outweighs potential  
2 difficulties in management of this class action.

3 83. Plaintiff knows of no special difficulty to be encountered in the maintenance of  
4 this action that would preclude its maintenance as a class action.  
5

## 6 VI. CLAIMS FOR RELIEF

### 7 COUNT ONE — 8 VIOLATION OF SECTION 15(A) OF ILLINOIS'S BIOMETRIC INFORMATION 9 PRIVACY ACT (740 ILCS 14/15(A)) BY FAILING TO ESTABLISH A PUBLICLY 10 AVAILABLE POLICY GOVERNING THE RETENTION OF BIOMETRIC 11 IDENTIFIERS AND INFORMATION

12 84. Plaintiff repeats and incorporates by reference all preceding paragraphs and  
13 allegations.  
14

15 85. Section 15(a) of BIPA provides that “[a] private entity in possession of biometric  
16 identifiers or biometric information must develop a written policy, made available to the public,  
17 establishing a retention schedule and guidelines for permanently destroying biometric identifiers  
18 and biometric information . . . .”<sup>74</sup> The biometric identifiers and information must be  
19 permanently destroyed “when the initial purpose for collecting or obtaining such identifiers or  
20 information has been satisfied or within 3 years of the individual’s last interaction with the  
21 private entity, whichever occurs first.”<sup>75</sup>  
22

23 86. Amazon is a Delaware corporation and is therefore a “private entity” under  
24 BIPA.<sup>76</sup>  
25

---

26 <sup>74</sup> 740 ILCS 14/15(a).

<sup>75</sup> 740 ILCS 14/15(a).

<sup>76</sup> 740 ILCS 14/10.

87. The facial geometries of Plaintiff and Class Members are “biometric identifiers” under the Act, and the information that Amazon derived from these identifiers is “biometric information” covered by the Act.<sup>77</sup>

88. As explained in paragraphs 55 to 60 above, Amazon did not properly develop a publicly available written policy governing the retention of biometric identifiers and information.

89. By improperly retaining the biometric information of Plaintiff and Class Members, Amazon violated the very privacy interests that BIPA was intended to protect.

90. On behalf of themselves and the Class, Plaintiff seeks:

A. injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Amazon to develop and make publicly available a retention policy that complies with BIPA’s § 15(a);<sup>78</sup>

B. the greater of liquidated damages of \$5,000 or actual damages for each of Amazon’s intentional or reckless violations of § 15(a);<sup>79</sup>

C. the greater of liquidated damages of \$1,000 or actual damages for each of Amazon’s negligent violations of § 15(a);<sup>80</sup> and

D. reasonable attorneys’ fees and costs and other litigation expenses.<sup>81</sup>

**COUNT TWO —  
VIOLATION OF SECTION 15(B) OF ILLINOIS’S BIOMETRIC INFORMATION  
PRIVACY ACT (740 ILCS 14/15(B)) BY OBTAINING BIOMETRIC IDENTIFIERS OR  
INFORMATION WITHOUT NOTICE OR CONSENT**

91. Plaintiff repeats and incorporates by reference all preceding paragraphs and allegations.

---

<sup>77</sup> *Id.*

<sup>78</sup> 740 ILCS 14/20(4).

<sup>79</sup> 740 ILCS 14/20(2).

<sup>80</sup> 740 ILCS 14/20(1).

<sup>81</sup> 740 ILCS 14/20(3).

92. Section 15(b) of BIPA makes it unlawful for any private entity to:

collect, capture, purchase, receive through trade, or otherwise obtain a person's . . . biometric identifier or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . .<sup>82</sup>

93. The "written release" required by § 15(b)(3) means "informed written consent."<sup>83</sup>

94. Amazon systematically and automatically collected, stored, and used Plaintiff's and Class Members' biometric identifiers and information without providing the notice required by § 15(b)—including notice that their biometric data was being used for the "specific purpose" of training Amazon's Rekognition technology.

95. Likewise, Amazon never obtained from Plaintiff or Class Members the informed written consent required by BIPA.

96. By improperly collecting, storing, and using Plaintiff's and Class Members' biometric identifiers and information, Amazon violated their rights to privacy in their biometric data.

97. On behalf of themselves and the Class, Plaintiff seeks:

A. injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Amazon to comply with § 15(b)'s requirement for collecting, storing, and using biometric identifiers and information;<sup>84</sup>

B. the greater of liquidated damages of \$5,000 or actual damages for each of Amazon's intentional or reckless violations of § 15(b);<sup>85</sup>

---

<sup>82</sup> 740 ILCS 14/15(b).

<sup>83</sup> 740 ILCS 14/10.

<sup>84</sup> 740 ILCS 14/20(4).

<sup>85</sup> 740 ILCS 14/20(2).

C. the greater of liquidated damages of \$1,000 or actual damages for each of Amazon's negligent violations of § 15(b);<sup>86</sup> and

D. reasonable attorneys' fees and costs and other litigation expenses.<sup>87</sup>

**COUNT THREE —  
VIOLATION OF SECTION 15(C) OF ILLINOIS'S BIOMETRIC INFORMATION  
PRIVACY ACT (740 ILCS 14/15(C)) BY PROFITING FROM BIOMETRIC  
IDENTIFIERS OR BIOMETRIC INFORMATION OBTAINED THROUGH AMAZON  
PHOTOS**

98. Plaintiff repeats and incorporates by reference all preceding paragraphs and allegations.

99. Section 15(c) of BIPA makes it unlawful for any "private entity in possession of a biometric identifier or biometric information" to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."<sup>88</sup>

100. Amazon had possession of Plaintiff's and Class Members' biometric identifiers and information and, without informing them, profited from their biometric identifiers and information by using that biometric data to train its Rekognition technology, which Amazon marketed and sold to businesses, governmental entities, and other organizations.

101. By profiting from its undisclosed use of Plaintiff's and Class members' biometric identifiers and information, Amazon violated the substantive privacy interests that BIPA protects.

102. On behalf of herself and the Class, Plaintiff seek:

A. injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Amazon to cease profiting from the use of their biometric identifiers and information;<sup>89</sup>

---

<sup>86</sup> 740 ILCS 14/20(1).

<sup>87</sup> 740 ILCS 14/20(3).

<sup>88</sup> 740 ILCS 14/15(c).

<sup>89</sup> 740 ILCS 14/20(4).

1 B. the greater of liquidated damages of \$5,000 or actual damages for each of  
2 Amazon's intentional or reckless violations of § 15(c);<sup>90</sup>

3 C. the greater of liquidated damages of \$1,000 or actual damages for each of  
4 Amazon's negligent violations of § 15(c);<sup>91</sup> and

5 D. reasonable attorneys' fees and costs and other litigation expenses.<sup>92</sup>

6 **COUNT FOUR —**  
7 **UNJUST ENRICHMENT**

8 103. Plaintiff repeats and incorporates by reference all preceding paragraphs and  
9 allegations.

10 104. Plaintiff and Class Members did not authorize Amazon to profit from their  
11 biometric identifiers and information by using this biometric data to train its Rekognition  
12 technology, which Amazon then sold to businesses, governmental entities, and other  
13 organizations.

14 105. Amazon appreciated, accepted and retained the benefit bestowed upon it under  
15 inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiff and  
16 Class Members as described herein.

17 106. Defendant Amazon profited from Plaintiff's and Class Members' biometric  
18 identifiers and information and did not provide full compensation for the benefit received from  
19 Plaintiff and Class Members.

20 107. Defendant Amazon obtained Plaintiff's and Class Members' biometric identifiers  
21 and information through inequitable means in that it obtained biometric data from Plaintiff and  
22 Class Members' in violation of Illinois law.  
23  
24

25  
26 

---

<sup>90</sup> 740 ILCS 14/20(2).

<sup>91</sup> 740 ILCS 14/20(1).

<sup>92</sup> 740 ILCS 14/20(3).



108. Plaintiff and Class Members have no adequate remedy at law.

109. Under the circumstances, it would be unjust and unfair for Defendant Amazon to be permitted to retain any of the benefits obtained from Plaintiff and Class Members and their biometric identifiers and information.

110. Under the principles of equity and good conscience, Defendant Amazon should not be permitted to retain the biometric identifiers and information belonging to Plaintiff and Class Members because Defendant unlawfully obtained the biometric identifiers and information.

111. Defendant Amazon should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received as a result of obtaining, collecting, storing, using, possessing and profiting off of Plaintiff and Class Members' biometric identifiers and information, including but not limited to the value of the intellectual property derived therefrom.

## VII. PRAYER FOR RELIEF

112. WHEREFORE, on behalf of herself and the Class, Plaintiff respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as a representative of the Class, and appointing her counsel as Class Counsel;

B. Declaring that Amazon's actions, as set out above, violate § 15(a), (b), and (c) of BIPA;

C. Awarding the greater of actual damages or statutory damages of \$5,000 per intentional or reckless violation of BIPA,<sup>93</sup> and the greater of actual damages or statutory damages of \$1,000 per negligent violation of the BIPA;<sup>94</sup>

---

<sup>93</sup> 740 ILCS 14/20(2).

<sup>94</sup> 740 ILCS 14/20(1).

1 D. Awarding injunctive and other equitable relief as is necessary to protect  
2 the interests of the Class, including, among other things, an order requiring  
3 Amazon to collect, store, and use biometric identifiers in compliance with BIPA;

4 E. Awarding Plaintiff and the Class their reasonable litigation expenses and  
5 attorneys' fees;

6 F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the  
7 extent allowable; and

8 G. Awarding such other and further relief as equity and justice may require.

### 9 **VIII. JURY DEMAND**

10 Plaintiff demands a trial by jury on all issues so triable.

11 DATED this 17th day of June, 2021.

12 KELLER ROHRBACK L.L.P.

13 By /s/ Dean Kawamoto

14 Dean Kawamoto, WSBA# 43850

15 Derek Loeser, WSBA# 24274

16 Gretchen Freeman Cappio, WSBA# 29576

17 Felicia Craick, WSBA# 54505

18 1201 Third Avenue, Suite 3200

19 Seattle, WA 98101

20 Tel: (206) 623-1900

21 Fax: (206) 623-3384

22 dkawamoto@kellerrohrback.com

23 dloeser@kellerrohrback.com

24 gcappio@kellerrohrback.com

25 fcraick@kellerrohrback.com

1 WEXLER WALLACE LLP  
2 Kenneth Wexler  
3 Justin N. Boley  
4 Zoran Tasić  
5 55 West Monroe St., Suite 3300  
6 Chicago, IL 60603  
7 Tel: (312) 346 2222  
8 Fax: (312) 346 0022  
9 kaw@wexlerwallace.com  
10 jnb@wexlerwallace.com  
11 zt@wexlerwallace.com

8 GUSTAFSON GLUEK PLLC  
9 Daniel E. Gustafson  
10 Karla M. Gluek  
11 David A. Goodwin  
12 Mickey L. Stevens  
13 120 South Sixth Street, Suite 2600  
14 Minneapolis, MN 55402  
15 Tel: (612) 333-8844  
16 Fax: (612) 339-6622  
17 dgustafson@gustafsongluek.com  
18 kgluek@gustafsongluek.com  
19 dgoodwin@gustafsongluek.com  
20 mstevens@gustafsongluek.com

16 STEPHAN ZOURAS, LLP  
17 Ryan F. Stephan  
18 James B. Zouras  
19 Haley R. Jenkins  
20 STEPHAN ZOURAS, LLP  
21 100 N. Riverside Plaza  
22 Suite 2150  
23 Chicago, Illinois 60606  
24 Tel: (312) 233-1550  
25 Fax: (312) 233-1560  
26 rstephan@stephanzouras.com  
jzouras@stephanzouras.com  
hjenkins@stephanzouras.com

1 TAUS, CEBULASH & LANDAU, LLP  
2 Kevin Landau  
3 Archana Tamoshunas  
4 TAUS, CEBULASH & LANDAU, LLP  
5 80 Maiden Lane, Suite 1204  
6 New York, NY 10038  
7 Tel: (212) 931-0704  
8 Fax: (212) 931-0703  
9 klandau@tcclaw.com  
10 atamoshunass@tcclaw.com

11 *Attorneys for Plaintiff and the Proposed Class*  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26